[REDACTED DOCUMENT]

AFFIDAVIT

I, Andrea Sciolino, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I have been a Special Agent of the Federal Bureau of Investigation ("FBI") since July 2017. I am currently assigned to the FBI's Boston, Massachusetts Field Office, where I investigate wire fraud, bank fraud, and money laundering, among other economic crimes. I have received on-the-job and FBI-sponsored training on these types of investigations, which has included training on the use of surveillance techniques and the execution of search, seizure, and arrest warrants. I have a Master's degree in accounting and hold an active Certified Public Accounting license.

2. As a federal agent, I am authorized to investigate violations of United States laws and to execute warrants issued under the authority of the United States.

3. I am currently investigating RAQUEL PENA ("PENA") for her involvement in various federal crimes, including wire fraud, conspiracy to commit wire fraud, and aggravated identity theft, in violation of Title 18, United States Code, Sections 1343, 1349, and 1028A, respectively (collectively the "TARGET OFFENSES").

4. I make this affidavit in support of applications for a criminal complaint, a warrant for PENA's arrest, and search warrants for PENA's person and the property located at 41 Market Street, Apartment B, Lawrence, Massachusetts ("the SUBJECT PREMISES").

5. Based on the facts as set forth in this affidavit, there is probable cause to believe that PENA has committed the TARGET OFFENSES, and that she and the SUBJECT PREMISES possess or contain, respectively, evidence, fruits, and instrumentalities of the TARGET OFFENSES as described in Attachment B to the proposed warrants.

6. The facts set forth in this affidavit are based upon my personal observations, my training and experience, and information obtained from various law enforcement personnel and witnesses. This affidavit is intended to show merely that there is sufficient probable cause to support the requested complaint, arrest warrant, and search warrants. It does not purport to set forth all of my knowledge of or investigation into this matter. Unless indicated otherwise, all conversations and statements described in this affidavit are related in substance and in part, any communications in Spanish are based on draft translations into English by an FBI-affiliated linguist, and all dates are approximate. The WhatsApp communications referenced in this affidavit were exchanged through a combination of texts and voice recordings, all of which were voluntarily provided to me for review by the witnesses described below.

THE STATUTES

7. 18 U.S.C. § 1028A(a)(1) (aggravated identity theft). The statute states in pertinent part: "Whoever, during and in relation to any felony violation enumerated in subsection (c) [including wire fraud], knowingly transfers, possesses, or uses, without lawful authority, a means of identification of another person . . . [commits an offense against the United States]."

8. 18 U.S.C. § 1343 (wire fraud). The statute states in pertinent part: "Whoever, having devised or intending to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises, transmits or causes to be transmitted by means of wire . . . in interstate or foreign commerce, any writings, signs, signals, pictures, or sounds for the purpose of executing such scheme or artifice . . . [commits an offense against the United States]."

9. 18 U.S.C. § 1349 (wire fraud conspiracy). The statute states in pertinent part: "Any person who attempts or conspires to commit any offense under this chapter [including wire

fraud] . . . the commission of which was the object of the attempt or conspiracy . . . [commits an offense against the United States]."

PROBABLE CAUSE THAT PENA COMMITTED THE TARGET OFFENSES

The Pandemic Unemployment Assistance Program

10. On March 27, 2020, the Coronavirus Aid, Relief, and Economic Security Act ("CARES Act") was signed into law. The CARES Act created a new temporary federal unemployment insurance program called Pandemic Unemployment Assistance ("PUA"). PUA provides unemployment insurance benefits for individuals who are not eligible for other types of unemployment benefits (*e.g.*, the self-employed, independent contractors, or gig economy workers). PUA provided payments for these benefits beginning on or after January 27, 2020 and ending before December 31, 2020, for a maximum period of 39 weeks. On or about December 27, 2020, recipients of PUA were granted 13 weeks of extended benefits. The American Rescue Act has now further extended PUA benefits through September 4, 2021.

11. The Massachusetts Department of Unemployment Assistance ("DUA") administers and manages the PUA program in the Commonwealth of Massachusetts. Massachusetts residents may apply to DUA for PUA benefits through an online portal over which they submit certain personally identifiable information ("PII").

12. The PUA claims submitted to DUA are processed on a server in Colorado. I understand that PUA claims cause wires to be transmitted to and/or from this Colorado-based server.

13. As part of the PUA application process, a claimant provides their first and last name, Social Security number ("SSN"), date of birth and a residential and mailing address. In addition, the claimant selects a preferred payment method: direct deposit or payment of their

benefit on to a debit card. The claimant also provides a phone number and an email address to be used by DUA to provide updates, contact the claimant, and for authentication purposes. The email address can also be used by the claimant to access their PUA claim account and, if necessary, to reset their claim account password. A claimant can choose one of three ways to meet DUA's two-factor authentication requirement: authentication app, text message, or email.

Overview of the PENA Conspiracy

14. As a result of information obtained from DUA, telecommunications and bank records, and interviews of Witnesses 1, 2, and 3, I have become aware of the following:

a. PENA possessed a notebook containing the PII of other individuals, including their names, SSNs, and addresses.

b. PENA used that PII to make fraudulent PUA claims.

c. PENA worked with her former roommate, CC1, to submit some of the fraudulent PUA claims.

d. PENA also worked with other individuals to submit fraudulent PUA claims, including PENA's former boyfriend, CC2, and her daughter's boyfriend, CC3.

e. PENA recruited other acquaintances to receive the proceeds of fraudulent PUA claims into their bank accounts, withdraw all or some portion of those funds, and give cash to PENA.

15. As described more fully below, the FBI has identified more than $300,000 in unemployment claims in May 2020 connected to PENA, including through electronic devices used at PENA's and CC1's residences.

Claims Submitted Using the 174 IP Address

PENA's Connection to the 174 IP Address

16. On or about May 3, 2020, a PUA claim was submitted to DUA using PENA's name, date of birth (xx/xx/1981), SSN (XXX-XX-XX75), Massachusetts driver's license number (SXXXXX916), and home address in Lawrence, Massachusetts (41 Market Street).[1] The PUA claim also listed PENA's cellular phone number (xxx-xxx-7532).[2] The claim was submitted from IP Address 174.62.196.62 ("the 174 IP Address").

17. PENA has used the 174 IP Address since at least 2017. According to records obtained from Apple, an Apple account linked to PENA's cellular phone number (xxx-xxx-7532) was created in or about October 2017 using the 174 IP Address.[3]

18. The 174 IP Address belongs to Comcast Cable Communications LLC ("Comcast"). Records obtained from Comcast reflect that the 174 IP Address was previously subscribed to by CC1, with a service address of 6 E. Laurel Street, Lawrence, Massachusetts, and telephone number XXX-XXX-0524.

---

[1] PENA's claim listed only her street address and did not include her specific unit (Apartment B).

[2] PENA reported this same telephone number and the address 41 Market Street, Apt. B, Lawrence, Massachusetts, to U.S. Customs and Border Protection on or about March 21, 2021. PENA's address has also been confirmed through Massachusetts public land records, which list PENA as the registered owner of the property located at 41 Market Street. Witness 2 also provided the same telephone number for PENA.

[3] The Apple account was associated with Apple ID raquelpena1203@icloud.com.

19. Witness 1 told investigators that PENA and CC1 are former roommates and that PENA and CC1 have worked together to file unemployment claims using other individuals' PII.

PENA and Witness 2

20. Witness 2 reported that she has overheard PENA talk to members of PENA's family about filing unemployment claims. Witness 2 also reported that PENA has asked Witness 2 and others for their bank account information. According to Witness 2, PENA said that, in exchange for Witness 2's providing bank account information, PENA would have money deposited into Witness 2's bank account as a gift.

21. Witness 2 agreed to PENA's proposal. Witness 2 and PENA discussed this transaction in text and audio WhatsApp communications (that Witness 2 shared with investigators) between on or about May 6 and on or about May 9, 2020. Those WhatsApp communications and records from DUA reveal that PENA and Witness 2 worked together to submit the fraudulent unemployment claim described below (the "Victim 1 Claim").

The Victim 1 Claim

22. On or about May 6, 2020, PENA told Witness 2 in a WhatsApp communication to expect money coming into Witness 2's bank account. PENA messaged the number "5536" and told Witness 2, "They are going to give you that. We're going to give the one that filled it out 500". PENA then clarified, "Five thousand for you".

23. DUA records reflect that on or about that same day, May 6, 2020, Claim A00-000-0252-4932 (the Victim 1 Claim) was submitted to DUA in the name and SSN of Victim 1. The claim stated that Victim 1 lived in Lawrence, Massachusetts and provided the email address [redacted]11@gmail.com. However, the claim used Witness 2's telephone 6

number and used Witness 2's Bank of America account information as the receiving bank account for the benefits. The claim was submitted from the 174 IP Address.

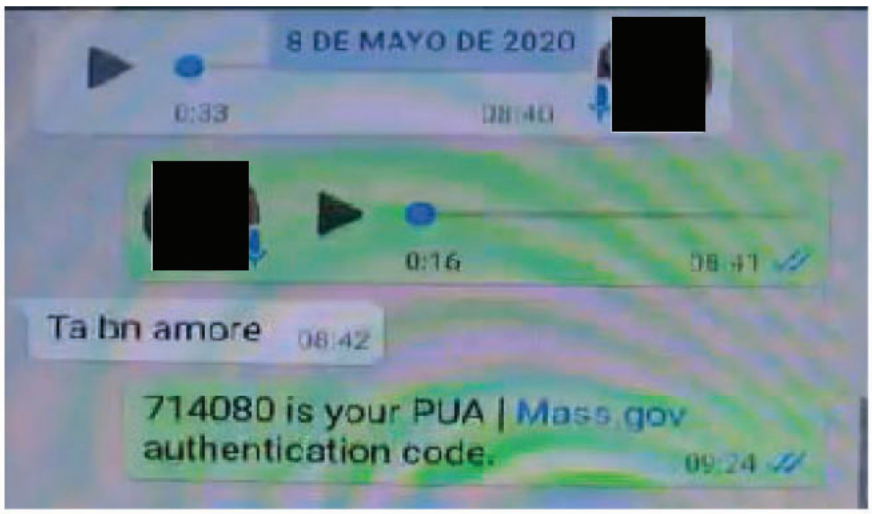
24. I have been unable to find any records for Victim 1 at the Lawrence, Massachusetts address provided to DUA.

25. On or about May 8, 2020, Witness 2 and PENA further discussed the Victim 1 Claim via WhatsApp text and audio messages. That discussion includes, in part, the following exchange:

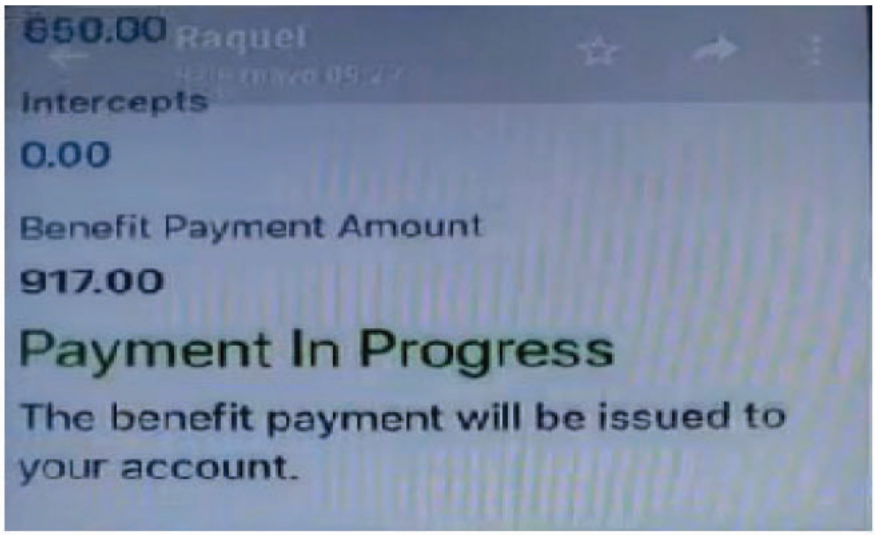
a. PENA said: "I'm going to check the account to see what happened. It was supposedly going to be deposited. Let's see if there-there-there-is something wrong, to fix it or do another one for you".

b. PENA then said: "[W]hen I try to enter the account, they are going to send you a code so that I can get in". PENA further stated that "in a little while I'm going to call you so that you send it [the code] to me and that way I can get in and be sure that they are going to deposit it for you".

c. Less than an hour later, Witness 2 sent PENA the "PUA / Mass.gov authentication code" that Witness 2 received, explaining, "I got that just now". This image contains the authentication code sent by Witness 2:



d. PENA responded, "Yes, that was it". PENA then sent a screenshot showing that the payment was in progress and told Witness 2, "It will go in tomorrow, for sure". The following image contains the screenshot PENA sent:



26. The next day, May 9, 2020, Witness 2 told PENA via WhatsApp, "The money came in" and "I'll give you the money later". PENA responded, "That's great, sweetie" and instructed Witness 2 to "Take it all out and stash it" and "Don't leave it in the bank".

27. Bank of America records for Witness 2's account reflect that $5,536 was deposited into Witness 2's account on May 11, 2020. The deposit references "Cares Act…… [Victim 1]".

Witness 2 told investigators that they withdrew money from their Bank of America account and gave some of that money to PENA; Bank of America records reflect a $5,000 withdrawal from Witness 2's bank account on or about May 11, 2020.

PENA and Witness 3

28. According to Witness 3, PENA learned in or about April 2020 that Witness 3 had received an unemployment assistance payment. PENA told Witness 3 that PENA was filing multiple unemployment assistance claims. PENA asked if Witness 3 would be willing to receive unemployment funds into Witness 3's bank account in exchange for what PENA described as a "gift". Witness 3 declined but agreed to find others who were interested in receiving funds for PENA.

29. On or about May 13, 2020, PENA told Witness 3, in a recorded WhatsApp conversation that Witness 3 shared with investigators, that "I [PENA] have here, like 40 or 50 numbers. You hear? If [CC3] is looking for accounts, I don't have to look for accounts outside. [CC3] has made a ton of money. Here, everyone is making – Here, no one has a need . . . ."

30. WhatsApp communications obtained in the investigation and records from DUA reveal that between on or about April 25, 2020 and on or about May 31, 2020, Witness 3 gave PENA information for multiple bank accounts, and PENA used that information to submit fraudulent unemployment claims, including the Victim 2 Claim and the Victim 3 Claim described below.

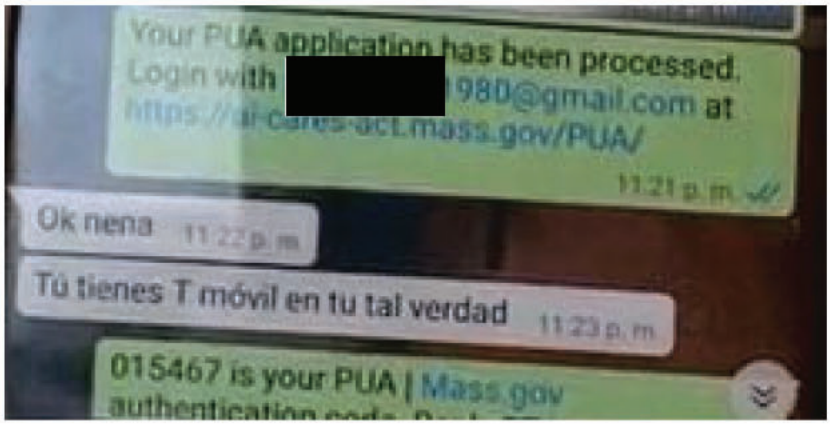
The Victim 2 Claim

31. On or about May 6, 2020, Witness 3 and PENA exchanged WhatsApp messages discussing the submission of an unemployment claim. That discussion includes, in part, the following exchange:

a. Witness 3 provided PENA the bank account information for a PNC Bank account (Account XXXXXXX563). After providing that information, Witness 3 instructed PENA, "Do it with that one first".

b. PENA responded by saying, "OK, love. I'm going to do it right now". PENA then instructed Witness 3 to "Be paying attention to your phone" and "Be ready. Everything you receive, send it to me".

c. Less than one hour later, Witness 3 responded with a screen shot showing that a "PUA Application has been processed" associated with the email "[redacted]1980@gmail.com". Witness 3 then provided PENA with the "PUA / Mass.gov authentication code". The following image contains both the screenshot and the authentication code PENA sent to Witness 3:



d. PENA responded, "Let me see if they accepted it". PENA then said, "5536 thousand. That's what is going to go in, sweetie".

32. DUA records reflect that on or about the same day, May 6, 2020, Claim A00-000-0209-6766 was submitted to DUA in the name and SSN of Victim 2 with an address in Lawrence, Massachusetts. The claim listed the email address [redacted]1980@gmail.com and PNC Bank account (Account XXXXXXX563), which are the same email address and bank

account that Witness 3 and PENA discussed by WhatsApp. The claim also listed Witness 3's telephone number and was submitted from the 174 IP Address.

33. In or about November 2020, law enforcement personnel interviewed Victim 2, who resides in Puerto Rico. Victim 2 confirmed that the SSN used in the Victim 2 Claim belonged to her. Victim 2 stated that she has never traveled outside Puerto Rico or filed for PUA benefits. Victim 2 did not recognize the email address used to submit the claim in [redacted]1980@gmail.com); nor did she know PENA or Witness 3.

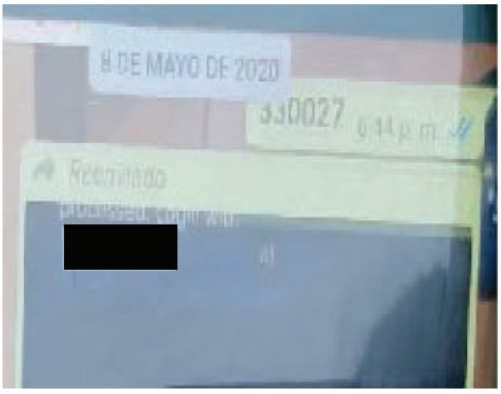
The Victim 3 Claim

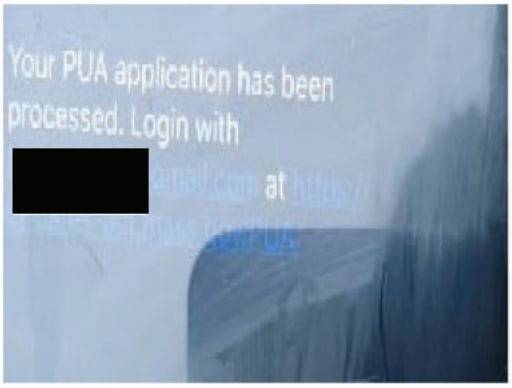
34. On or about May 8, 2020, Witness 3 and PENA exchanged WhatsApp messages discussing the submission of another unemployment claim. That discussion includes, in part, the following exchange:

a. PENA asked Witness 3, "Does he want me to do another one or should we wait for the one from last night?"

b. Witness 3 responded, "Do another one", and then provided PENA with a Digital Federal Credit Union account number (XXXXX161). After providing that information, Witness 3 gave PENA a telephone number.

c. Approximately three hours later, Witness 3 sent PENA a code number ("330027") and a photo containing the message, "Your PUA application has been processed" along with an email address containing Victim 3's first name. The following images contain the code number and a portion of the photo Witness 3 sent PENA:





d. PENA then told Witness 3, "5044. That's going to arrive".

35. DUA records reflect that on or about that same day, May 8, 2020, Claim A00-000-0310-0989 was submitted to DUA in the name and PII of Victim 3 using an address in Lawrence, Massachusetts. The claim listed both the bank account and phone number that Witness 3 and PENA discussed by WhatsApp messages. The claim was for $5,044, the same amount PENA told Witness 3 in their WhatsApp messages was "going to arrive". This claim was also submitted from the 174 IP Address.

36. In or about November 2020, law enforcement personnel interviewed Victim 3, who resides in Puerto Rico. Victim 3 confirmed that the SSN and date of birth used in the Victim 3 Claim were his. Victim 3 stated, however, that he had never lived in Massachusetts or filed for pandemic unemployment benefits. Victim 3 did not know PENA or Witness 3.

Claims Submitted Using the 73 IP Address

PENA's Connection to the 73 IP Address

37. The IP Address 73.119.135.4 (the "73 IP Address") belongs to Comcast. Comcast records reflect that it provides internet service through the 73 IP Address to 41A Market Street, Lawrence, Massachusetts.

38. Investigators have confirmed that PENA owns the building at 41 Market Street, and that the property is divided into two apartments, Apartment A and Apartment B:

a. In or about June 2018, 41 Market Street, Lawrence, Massachusetts was deeded to PENA, and a mortgage was taken out on the property in her name.

b. PENA owns a 2017 Honda that is registered in her name to 41 Market Street, Apt. B, Lawrence, Massachusetts (*i.e.*, the SUJBECT PREMISES).

c. PENA's driver's license lists 41 Market Street, Apt. B, Lawrence, Massachusetts (*i.e.*, the SUBJECT PREMISES) as her address.

d. On or about March 21, 2021, PENA reported to Customs and Border Protection that her address was 41 Market Street, Apt. B, Lawrence, Massachusetts (*i.e.*, the SUBJECT PREMISES).

e. Witness 1 confirmed that PENA lives in the SUBJECT PREMISES (*i.e.*, Apartment B) and that the internet is shared between Apartment A and the SUBJECT PREMISES.

39. Witness 1's statement regarding the shared internet service between Apartment A and the SUBJECT PREMISES is corroborated by records from Apple, which show that PENA's cellular phone (xxx-xxx-7532) connected to her Apple account using the 73 IP Address on hundreds of occasions in 2020. For example, PENA's cellular phone received over 200 iTunes Updates using the 73 IP Address between January 6, 2020 and June 29, 2020.

Claims Connected to Witness 1's Bank Account and PENA's Cellular Phone

40. Witness 1 provided investigators with information about how PENA worked with CC1, CC2, and CC3 to submit unemployment claims. Witness 1 said that CC3 originally filed

unemployment claims via computer. But Witness 1 also heard PENA and CC3 discuss using cellular telephones to file claims.

41. According to Witness 1, CC2 told Witness 1 that it was originally CC2's idea to use PENA's notebook of PII to file unemployment claims. CC2 also told Witness 1 that CC2 needed people to receive the payments from the unemployment claims into their bank accounts and that those people could keep some of the money from those payments.

42. Witness 1 agreed to receive unemployment payments into Witness 1's bank account. Witness 1 told investigators that Witness 1's bank account received multiple unemployment payments and that Witness 1 was able to keep approximately $6,000 in profit.

43. Records from TD Bank reflect that Witness 1 has an account there (Account XXXXXXX291). DUA records confirm that Witness 1's TD Bank account received payments on at least two PUA claims that were submitted using the 73 IP Address in the name of a third party, as set forth below:

a. On or about May 8, 2020, DUA received claim A00-000-0295-5367 in the name of Victim 4. The address listed was on Walnut Avenue in Revere, Massachusetts.

b. On or about May 17, 2020, DUA received claim A00-000-0408-2533 in the name of Victim 5. The address listed was on Royal Street in Lawrence, Massachusetts.

44. DUA records also reflect that, in addition to the claims paid into Witness 1's bank account, the 73 IP Address was used in or about May 2020 to submit two claims that listed PENA's cellular phone number (xxx-xxx-7532) but the names of individuals other than PENA:

a. On or about May 6, 2020, DUA received claim A00-000-0235-8869 in the name of Victim 6. The address listed was on Lowell Street in Methuen, Massachusetts. In or about November 2020, investigators interviewed Victim 6, a resident of Puerto Rico, who said that he had never worked or lived in Massachusetts, never applied for unemployed benefits, and did not know PENA.

b. On or about May 10, 2020, DUA received claim A00-000-0224-9753 in the name of Victim 7. The address listed was 41 Market Street, Lawrence, Massachusetts (PENA's property).

Total Claims Submitted from the 174 IP Address and the 73 IP Address in May 2020

45. DUA records reflect that the 174 IP Address, subscribed to by CC1, was used in or about May 2020 to submit approximately 28 PUA claims. While some of those claims were denied, the total amount paid out on these claims was approximately $144,000.

46. DUA records also reflect that the 73 IP Address, assigned to PENA's building and shared with the SUBJECT PREMISES, was used in or about May 2020 to submit approximately 21 PUA claims. While some of those claims were denied, the total amount paid out on these claims was approximately $172,800.[4]

Continuing Nature of the PENA Scheme

47. There is probable cause to believe that the SUBJECT PREMISES, PENA's cellular phone and email accounts, continue to be used as instrumentalities of the TARGET OFFENSES.

[4] The claim amounts for the 174 IP Address and the 73 IP Address do not include claims filed in the names of PENA, CC1, CC2, CC3, Witness 1, Witness 2, or Witness 3.

DUA records reflect that the 73 IP Address has been used to login to DUA's PUA web portal in January and February of 2021. For example, the 73 IP Address has logged into DUA's PUA web portal on claims made in the following names (and PUA claim numbers):

a. Victim 8 (A00-000-1535-2875). A login occurred from the 73 IP Address on or about January 10, 2021. The claim was initially submitted on or about December 12, 2020 using the 73 IP Address. But the address provided to DUA on this claim was on Bellevue Avenue in Haverhill, Massachusetts, and I have been unable to find any record that Victim 8 resides at the 41 Market Street address.

b. Victim 9 (A00-000-0320-0235). Logins to this claimant's account occurred from the 73 IP Address on or about January 10 and 24, 2021. The claim was initially submitted on or about May 12, 2020 using the 73 IP Address. But the address provided to DUA on this claim was on Exeter Street in Lawrence, Massachusetts. Further, Victim 9 currently resides in Puerto Rico and told investigators that she does not know PENA and has never filed for unemployment. Benefits continue to be paid on this claim, including a payment for $567.00 on or about March 15, 2021.

c. Victim 10 (A00-000-0360-8593). Logins to this claimant's account occurred from the 73 IP Address on or about January 10 and 24, 2021. The claim was initially submitted on or about May 15, 2020 using the 73 IP Address. But the address provided to DUA on the claim was on Bedford Street in Methuen, Massachusetts, and I have been unable to find any record that Victim

10 resides at the 41 Market Street address. Benefits continue to be paid on this claim, including a payment for $567.00 on or about March 15, 2021.

d. Victim 11 (A00-000-0132-8277). Logins to this claimant's occurred from the 73 IP Address on or about January 9, 12, and 17, and on February 15, 2021. While this claim was initially submitted on or about April 30, 2020 from a different IP Address,[5] the claim listed PENA's address (41B Market Street, the SUBJECT PREMISES), PENA's cellphone number (xxx-xxx-7532), and an email address in PENA's name. I have been unable to find any record that Victim 11 resides at the 41 Market Street address. Benefits continue to be paid on this claim, including a payment for $567.00 on or about March 15, 2021.

48. For each of these logins, DUA would have required dual factor authentication. As noted above, DUA sends authentication messages through one of three avenues: text message to the phone number on file, email to the email address on file, or through DUA's authentication app.

49. I am aware that in or about February 2021, DUA mailed 1099-G tax forms to the addresses on file for PUA claimants, and that, as recently as March 2021, it sent "Notice[s] of Monetary Redetermination" when it extended PUA benefits. DUA sent these communications to the email address and/or mailing address on file for each PUA claim.

50. Based on the foregoing, there is probable cause to believe that PENA and others known and unknown have accessed DUA's PUA web portal using the 73 IP Address, including as

[5] DUA records reflect that this claim was originally submitted using IP Address 96.230.105.5.

recently as February 2021, and that PENA has received DUA communications via mail and email, and on her cellular phone, including as recently as March 2021.

EVIDENCE, FRUITS, AND INSTRUMENTALITIES OF THE TARGET OFFENSES

51. There is accordingly probable cause to believe that PENA and the SUBJECT PREMISES, identified in the respective Attachments A to the proposed warrants, possess or contain fruits, evidence, and instrumentalities of the TARGET OFFENSES as described in Attachment B to the proposed warrants.

52. As described more fully above, PENA and others known and unknown have used the property located at 41 Market Street, Lawrence, MA, 01843 and the 73 IP Address to submit fraudulent unemployment claims. PENA owns the entire 41 Market Street property. From both personal observation and multiple public sources, I can confirm that the 41 Market Street property is a stand-alone, two-story structure with a finished basement that is subdivided into two units, Apartment A and Apartment B. PENA resides in Apartment B. PENA's residential address has been identified through, for example, car registration and driver's license records. Additionally, on or about March 21, 2021, PENA confirmed her residential address and cellphone number to Customs and Border Protection.

53. Because the internet is shared between Apartment A and the SUBJECT PREMISES, a device accessing DUA's network in furtherance of fraudulent claims from the 73 IP Address could have been in either Apartment A or the SUBJECT PREMISES. This affidavit,

however, only seeks authority to search the SUBJECT PREMISES (*i.e.*, Apartment B), where PENA resides.[6]

54. For the reasons noted above, there is probable cause to believe that DUA has mailed multiple PUA-related letters to PENA's 41 Market Street property, including to the SUBJECT PREMISES, because PENA and others known and unknown have listed the SUBJECT PREMISES on PUA claims submitted to DUA. These included the Victim 11 claim, which was submitted using PENA's cellular phone number (xxx-xxx-7532). PENA has therefore likely received mail from DUA at her 41 Market Street property and the SUBJECT PREMISES, including mail related to one or more claims submitted in the name and PII of third parties. PENA would have also received communications on her cellphone, which based on my training and experience and through information obtained during this investigation, PENA regularly keeps on her person.

55. There is also probable cause to believe that PENA possesses information, either on her person or at the SUBJECT PREMISES, used to submit fraudulent PUA claims. PENA and others known and unknown have submitted fraudulent PUA claims from 41 Market Street and the 73 IP Address. A PUA claimant typically provides a substantial amount of information when submitting a PUA claim, including a first and last name, date of birth, phone number, residential and mailing address, email address, SSN, and bank account information. Because they submitted so many claims, PENA and others known and unknown likely wrote down or preserved at least

---

[6] [redacted] resided and may continue to reside in Apartment A, but this fact does not negate the probable cause to believe that the SUBJECT PREMISES will contain evidence, fruits, and instrumentalities of the TARGET OFFENSES. Most notably, PENA and PENA's cell phone are both closely linked to the 73 IP Address and the filing of fraudulent claims, including claims that did not involve [redacted]

some of this information. The email address used to submit the claims, for example, would have to be retained in order to later login to DUA's PUA web portal. Further, Witness 1 reported to investigators that PENA had previously kept a black notebook that contained third-party PII. PENA later claimed that she removed the notebook from her residence. However, based on training and experience, I know that individuals often lie about whether and how they have disposed of evidence of their crimes. Further, based on my training and experience, there is probable cause to believe that PENA kept PII used to submit fraudulent PUA claims because that information retains value for other criminal schemes. In addition to PENA's unemployment fraud scheme described above, PII can be sold or used for identity fraud, fraudulent loans or money transfers, counterfeit credit cards, and/or blackmail and extortion. Based on my training and experience, individuals tend to store valuable information, including PII, in a private location, such as their residence or on their smartphone.

Seizure of Computer Equipment and Data

56. The investigation has determined that fraudulent unemployment claims were submitted online to DUA using mobile phones and/or computers. Some of those submissions were made from the 41 Market Street property using the 73 IP Address. Recent logins to DUA's PUA web portal have also occurred from the 73 IP Address. Records obtained from Apple reflect that PENA owned an Apple iPhone version 11.6. Records from Apple also reflect that PENA's Apple iCloud account utilized the "back up" service over the 73 IP Address in June 2020. Additionally, Witness 1 said that CC3, who reportedly lived at the SUBJECT PREMISES,[7] originally filed unemployment claims via computer, and Witness 1 also

[7] PUA claim A00-000-0069-8357 was submitted to DUA on April 30, 2020 in the name of CC3 and listed the SUBJECT PREMISES as his address.

heard PENA and CC3 discuss using cellular telephones to file claims. Email addresses were also created and telephone numbers were used to file the claims and to receive confirmation codes in order to access and process the fraudulent unemployment claims. PUA claims submitted in the name of PENA and others have listed PENA's cellular phone number as a means of receiving communications from DUA.

57. Additionally, from my training, experience, and information provided to me by other agents, I am aware that individuals frequently also use computers to create and store records of their actions by communicating about them through email, instant messages, and updates to online social networking websites; drafting letters; keeping their calendars; arranging for travel; storing pictures; researching topics of interest; buying and selling items online; and accessing their bank, financial, investment, utility, and other accounts online. Many cell phones, such as the Apple iPhone, now function essentially as small computers. Phones have capabilities that include serving as a wireless telephone to make audio calls, digital camera, portable media player, GPS navigation device, sending and receiving text messages and emails, and storing a range and amount of electronic data. Examining data stored on devices of this type can uncover, among other things, evidence of communications and evidence that reveals or suggests who possessed or used the device. For example, PENA's WhatsApp messages obtained during this investigation demonstrate that PENA used her cellular phone to discuss and facilitate the submission of fraudulent unemployment claims, including through the exchange of texts, audio notes, and pictures.

58. Information stored within a computer and other electronic storage media may also provide crucial additional evidence of the "who, what, why, when, where, and how" of the TARGET OFFENSES, thus enabling the United States to establish and prove each element of the TARGET OFFENSES, or alternatively, to exclude the innocent from further suspicion.

Information stored within a computer or storage media (*e.g.*, registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can provide, for example:

a. Evidence of who has used or controlled the computer or storage media and what computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may also indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner.

b. Evidence of how and when the computer or storage media was accessed or used. Computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation.

c. Evidence relating to the physical location of other evidence and the suspect. Images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the

presence of additional electronic storage media (*e.g.*, a digital camera or cellular phone with an incorporated camera).

d. Information within the computer may indicate the owner's motive and intent to commit a crime (*e.g.*, internet searches indicating criminal planning), or consciousness of guilt (*e.g.*, running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

59. From my training, experience, and information provided to me by other agents, I am aware that individuals commonly store records of the type described in Attachment B to the proposed warrant in computer hardware, computer software, smartphones, and storage media. Further, computer files or remnants of such files can be recovered months or years after they have been written, downloaded, saved, deleted, or viewed locally or over the Internet. This is true because:

a. Electronic files that have been downloaded to a storage medium can be stored for years at little or no cost. When users replace their computers, they can easily transfer the data from their old computer to their new computer.

b. Even after files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data, which might not occur for long periods of time. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media contain electronic evidence of how the computer has been used, what it has been used for, and who has used it. This evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. It is technically possible to delete this information, but computer users typically do not erase or delete this evidence because special software is typically required for that task.

d. Similarly, files that have been viewed over the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache." The browser often maintains a fixed amount of hard drive space devoted to these files, and the files are overwritten only as they are replaced with more recently viewed Internet pages or if a user takes steps to delete them.

e. Data on a storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, email programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record

information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

60. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

61. The law enforcement agents will endeavor to search and seize only the computer equipment which, upon reasonable inspection and/or investigation conducted during the execution of the search, reasonably appear to contain the evidence in Attachment B to the proposed warrant because they are associated with (*i.e.*, used by or belong to) PENA, CC1, CC2, and/or CC3. However, there may be computer equipment identified during the search whose association with PENA, CC1, CC2, CC3 is not possible to determine at the scene. Computer equipment and data can be disguised, mislabeled, or used without the owner's knowledge. In addition, technical, time, safety, or other constraints can prevent definitive determination of their ownership at the premises during the execution of the proposed warrant. Therefore, if the law enforcement agents cannot make a determination as to use or ownership regarding any particular device, this application seeks permission to search and seize all electronic devices if the things described in Attachment B to the proposed warrant are of the type that might be found on those devices.

62. This application further seeks to conduct the search and seizure onsite or off-site in order to determine their true use or contents, regardless of how the contents or ownership appear or are described by people at the scene of the search. Based on my knowledge and training and the experience of other agents with whom I have spoken, I am aware that in order to completely and accurately retrieve data maintained in computer hardware, computer software or storage media, to ensure the accuracy and completeness of such data, and to prevent the loss of the data

either from accidental or programmed destruction, it is often necessary that computer hardware, computer software, and storage media be seized and subsequently processed by a computer specialist in a laboratory setting rather than in the location where it is seized. This is true because:

a. The volume of evidence storage media such as hard disks, flash drives, CDs, and DVDs can store the equivalent of thousands or, in some instances, millions of pages of information. Additionally, a user may seek to conceal evidence by storing it in random order or with deceptive file names. Searching authorities may need to examine all the stored data to determine which particular files are evidence, fruits, or instrumentalities of criminal activity. This process can take weeks or months, depending on the volume of data stored, and it would be impractical to attempt this analysis on-site.

b. Technical requirements analyzing computer hardware, computer software or storage media for criminal evidence is a highly technical process requiring expertise and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications. Thus, it is difficult to know, before the search, which expert possesses sufficient specialized skill to best analyze the system and its data. Furthermore, data analysis protocols are exacting procedures, designed to protect the integrity of the evidence and to recover even "hidden," deleted, compressed, or encrypted files. Many commercial computer software programs also save data in unique formats that are not conducive to standard data searches. Additionally, computer evidence is extremely vulnerable to tampering or destruction, both from external sources and destructive code imbedded in the system as a "booby trap."

Consequently, law enforcement agents may either copy the data at the premises to be searched or seize the computer equipment for subsequent processing off-site.

63. Off-site processing may also be necessary because the process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the proposed warrant.

Unlocking a Device Using Biometric Features

64. I know from my training and experience, as well as from information found in publicly available materials, that some models of cellphones made by Apple and other manufacturers, offer their users the ability to unlock a device via the use of a fingerprint or through facial recognition, in lieu of a numeric or alphanumeric passcode or password.

65. On the Apple devices that have this feature, the fingerprint unlocking feature is called Touch ID. If a user enables Touch ID on a given Apple device, he or she can register up to 5 fingerprints that can be used to unlock that device. The user can then use any of the registered fingerprints to unlock the device by pressing the relevant finger(s) to the device's Touch ID sensor. In some circumstances, a fingerprint cannot be used to unlock a device that has Touch ID enabled, and a passcode must be used instead, such as: (1) when more than 48 hours has passed since the last time the device was unlocked and (2) when the device has not been unlocked via Touch ID in 8 hours and the passcode or password has not been entered in the last 6 days. Thus, in the event

law enforcement encounters a locked Apple device, the opportunity to unlock the device via Touch ID exists only for a short time. Touch ID also will not work to unlock the device if (1) the device has been turned off or restarted; (2) the device has received a remote lock command; or (3) five unsuccessful attempts to unlock the device via Touch ID are made.

66. The passcode that would unlock any of PENA's devices found during the search of the Subject Premises is not currently known to law enforcement. Thus, it may be useful to press PENA's finger(s) to the device's fingerprint sensor or to hold the device up to PENA's face in an attempt to unlock the device for the purpose of executing the search authorized by this warrant. The government may not otherwise be able to access the data contained on those devices for the purpose of executing the search authorized by the proposed warrant.

67. For these reasons, I request that the Court authorize law enforcement to press the fingers (including thumbs) of PENA to the sensor of the devices or to place the devices in front of her face for the purpose of attempting to unlock the device in order to search the contents as authorized by the proposed warrant.

CONCLUSION

68. Based on the information described above, there is probable cause to believe that that PENA has violated the TARGET OFFENSES.

69. Based on the information described above, there is also probable cause to believe that evidence, fruits, and instrumentalities of the TARGET OFFENSES, as described in Attachment B to the proposed warrants, are contained within the SUBJECT PREMISES or on the person described in Attachment A to the proposed warrants.

Respectfully submitted,

Andrea Sciolino 4/1/21

ANDREA SCIOLINO
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me by telephone ~~or other reliable electronic means~~ under Fed. R. Crim. P. 4.1 on Apr 1, 2021 5:04 p.m.

David H. Hennessy

Honorable David H. Hennessy
United States Magistrate Judge